

رمزنگاری کلید عمومی RSA

سیستم رمزنگاری کلید عمومی RSA (آراس‌ای) یکی از قدیمی‌ترین و جذاب‌ترین‌هاست، و در این مطلب می‌خوایم تاریخچه، کاربرد، و اهمیتش در امنیت اطلاعات رو با هم مرور کنیم. با معرفی RSA در ۱۹۷۷، دنیای رمزنگاری وارد عصر جدیدی شد. خیلی از ما، ازجمله من، چهار دهه بعد از خلقش باهاش آشنا می‌شیم.

به‌طورکلی، دو نوع رمزنگاری داریم: متقارن (symmetric) و نامتقارن (asymmetric). در رمزنگاری متقارن، از یه کلید هم برای رمزنگاری و هم برای رمزگشایی استفاده می‌شه، به این معنا که فرستنده و گیرنده هر دو به یه کلید مشترک دسترسی دارن، و این، در بعضی موارد استفاده، می‌تونه ضعف محسوب بشه.

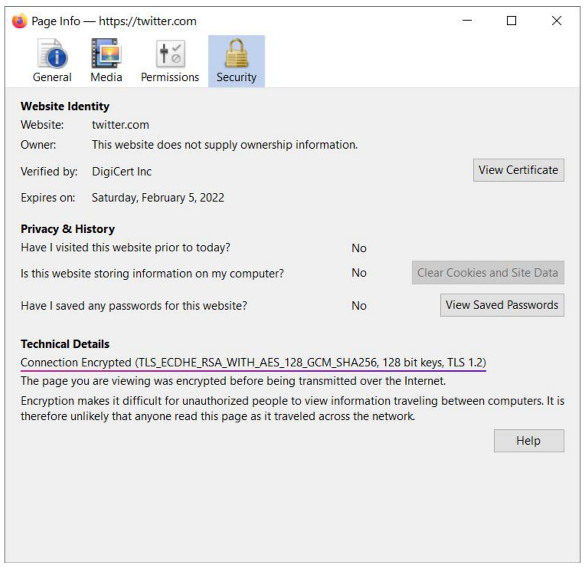


رمزنگاری نامتقارن فرآیند پیچیده‌تری داره: دو کلید دارید، یکی عمومی و دیگری خصوصی.

رمزنگاری کلید عمومی

در این روش، شما با استفاده از کلید عمومی خودتون چیزی رو رمزنگاری می‌کنید، و اون پیام یا داده تنها با کلید خصوصی مرتبط قابل‌رمزگشاییه. درحالی‌که این دو کلید یکی نیستن و با هم فرق دارن، از طریق ریاضی به هم مرتبطن.

رمزنگاری نامتقارن (یا رمزنگاری کلید عمومی) امنیت بسیار خوبی رو ارائه می‌ده، از این جهت که رسیدن به رابطهٔ بین دو کلید و پیداکردن کلید خصوصی دشواره—به لطف تابع یه‌طرفه‌ای که جلوتر بهش می‌پردازیم. از طرفی، رمزنگاری نامتقارن روش کندتری در مقایسه با رمزنگاری متقارن به‌حساب میاد.



یکی از رایج‌ترین الگوریتم‌های رمزنگاری متقارن AES (استاندارد رمزنگاری پیشرفته) است. همین الآن مرورگر شما برای اتصال امن به توئیتر از این نوع رمزنگاری استفاده می‌کنه.



معرفی AES در یوتیوب

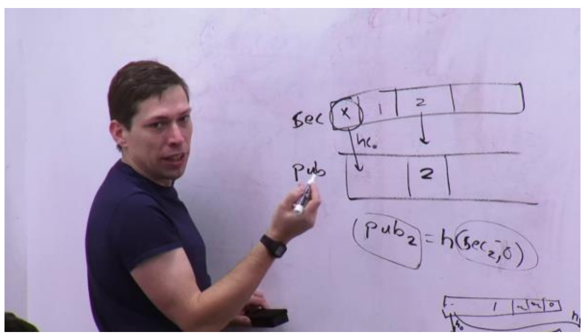


«۱۲۸ بیتی یا ۲۵۶ بیتی؟» تفاوت امنیت کلیدها در یوتیوب

وقتی راجع به رمزنگاری متقارن صحبت می‌کنیم، طول کلید در ارائهٔ امنیت بیشتر مهم و تأثیرگذاره، اما تنها فاکتور نیست. کلیدها در این نوع رمزنگاری—متشکل از رشته‌ای از حروف و اعداد—به‌طورمعمول ۱۲۸، ۱۹۲، و ۲۵۶ بیتی‌ان. ویدئوهای صفحهٔ قبل رو برای آشنایی بیشتر با تفاوت امنیت کلیدها ببینید.

طول کلیدها در رمزنگاری کلید عمومی بسیار بلندتره (۲۰۴۸ بیت به بالا)، اما روش سنجش امنیتش از رمزنگاری متقارن متفاوته. برای مثال، یه کلید عمومی ۳۰۷۲ بیتی از نظر امنیت کم‌وبیش با یه کلید ۱۲۸ بیت AES برابره. درموردش بخونید. (کلیدواژه‌ها: طول کلید (key size)، سطح امنیت (security level))

دو نمونه از سیستم‌های نامتقارن RSA و ECC (رمزنگاری منحنی بیضوی) هستن. اولی موضوع صحبت ماست، و دومی سیستمیه که در بیت‌کوین به‌کار رفته و کلیدهای عمومی و خصوصی شما بر پایه‌ش ساخته می‌شن.



رمزنگاری منحنی بیضوی در یوتیوب

سیستم رمزنگاری RSA

سیستم RSA اسم خودش رو از نام خانوادگی سه شخصی گرفته که در اختراعش نقش داشتن: ریوست، شامیر، و آدلمن.



سال ۱۹۷۶، ویتفیلد دیفی و مارتین هلمن ایدهٔ رمزنگاری نامتقارن رو مطرح کردن—ایده‌ای نو و انقلابی—اما راه‌حل عملی‌ای براش ارائه ندادن.

ریوست، شامیر، و آدلمن هر سه در ام‌آی‌تی تدریس می‌کردن، و ارتباط نزدیکی با هم داشتن. روزی یکی از شاگردهای ریوست مقالهٔ دیفی-هلمن رو بهش نشون می‌ده و می‌گه، «ممکنه برات جالب باشه»، و واقعاً بود. ریوست و شامیر، که در حوزهٔ کامپیوتر فعالیت داشتن، تصمیم می‌گیرن روی این مسئله کار کنن.

این دو ماه‌ها تلاش می‌کنن تابع یه‌طرفه‌ای رو پیدا کنن که محاسبه‌ش از یه سمت سریع اما از سمت دیگه بسیار سخت باشه، و درعین‌حال ضعف امنیتی‌ای نداشته باشه که برگشت‌پذیری‌اش رو ساده کنه. آدلمن، که ریاضی‌دان بود، مسئولیت این رو داشت که توابع پیشنهادی رو بشکنه و نقاط ضعفشون رو پیدا کنه.

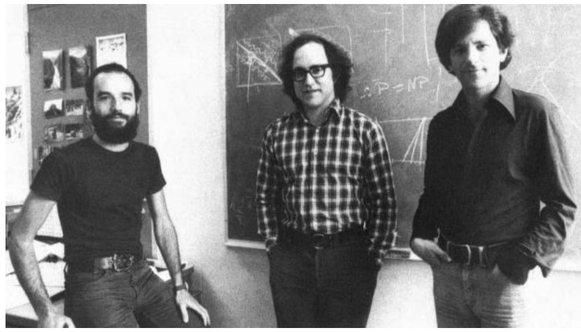


مرور تاریخچهٔ RSA با لئونارد آدلمن در یوتیوب

شبی در آوریل ۱۹۷۷، این سه توسط یکی از دانشجوها به مهمونی پِسَح (عیدی یهودی) دعوت می‌شن. بعد از برگشتن به خونه‌هاشون، ریوست، که خوابش نمی‌بره، شروع می‌کنه به کار روی مسئله و بالاخره تابع یه‌طرفه رو پیدا می‌کنه. به آدلمن زنگ می‌زنه، مطرحش می‌کنه، و آدلمن همونجا بهش تبریک می‌گه. ریوست تمام شب رو بیدار می‌مونه و تا صبح مقاله‌ش رو می‌نویسه.

داستان انتخاب اسم RSA هم یکی از اون چیزهاییه که شانسی اما فوق‌العاده اتفاق می‌افته. ریوست ابتدا قصد داشت نویسنده‌های مقاله رو به‌ترتیب معمول «آدلمن، ریوست، شامیر» بنویسه، اما آدلمن، که حس می‌کرد بیشتر کار رو اون‌ها انجام دادن، موافق نبود اسمش لحاظ بشه. درنهایت، بعد از کلی صحبت و فکر، قبول می‌کنه اما می‌گه اسم من رو آخر بذارید، و این‌طوری RSA خلق می‌شه.

ریوست، شامیر، و آدلمن سال ۲۰۰۲ جایزهٔ تورینگ (بالاترین جایزه در حوزهٔ کامپیوتر و به‌نوعی نوبل علوم کامپیوتر) رو به‌خاطر عملی‌ساختن رمزنگاری کلید عمومی بردن.



در این عکس معروف، یه شوخی بامزه روی تخته هست، که ریوست می‌گه احتمالاً من نوشتم. (درمورد مسئلهٔ برابری پی و ان‌پی بخونید.) اگه علاقه‌مندید با ریوست و کارهاش آشنا بشید، «تاریخ شفاهی رونالد ریوست» رو ببینید. به‌طبع، مصاحبهٔ کامل آدلمن با ACM (انجمن اعطاکنندهٔ جایزهٔ تورینگ) رو هم پیشنهاد می‌کنم.

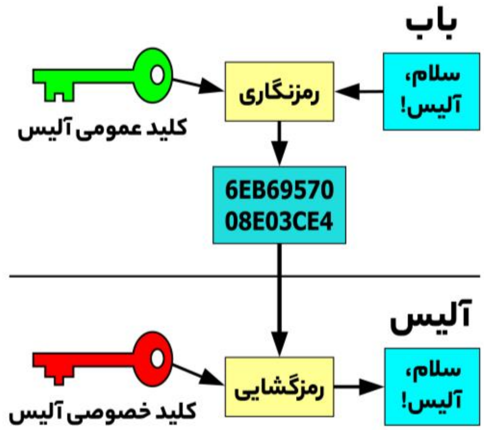
عملکرد RSA

اما RSA دقیقاً چطوری کار می‌کنه؟

با RSA، شما یه کلید عمومی و یه کلید خصوصی دارید. کلید عمومی رو می‌تونید دراختیار همه قرار بدید. می‌تونید اون رو در سایت شخصی خودتون بذارید، در امضای ایمیل، در بایوی توئیتر، یا روی کارت ویزیت. هرچیزی که با کلید عمومی شما رمزنگاری بشه، تنها با کلید خصوصی شما قابل‌رمزگشاییه.

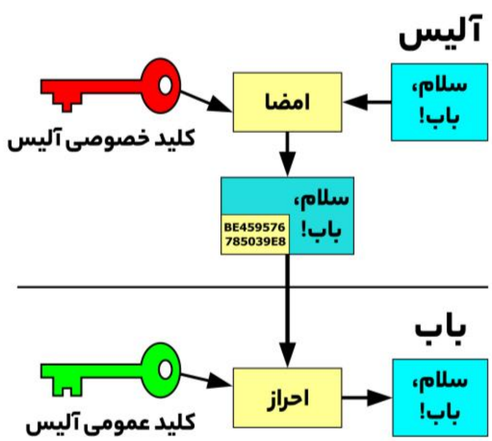
افراد می‌تونن از کلید عمومی شما برای ارسال پیامی محرمانه استفاده کنن، و اون شخص و شما می‌تونید مطمئن باشید کسی جز شما (دارندهٔ کلید خصوصی مرتبط با اون کلید عمومی) قادر به خوندن پیام نیست.

رمزنگاری و رمزگشایی



به این مثال توجه کنید. باب می‌خواد پیامی رو برای آلیس ارسال کنه اما نمی‌خواد کسی جز آلیس از محتوای پیام باخبر بشه. پیام خودش رو با «کلید عمومی آلیس» رمزنگاری می‌کنه. باب پیام رمزنگاری‌شده رو برای آلیس ارسال و آلیس با داشتن «کلید خصوصی» خودش می‌تونه اون رمزگشایی کنه و بخونه.

اصالت‌سنجی/احراز هویت



رمزنگاری کلید عمومی همچنین امکان اصالت‌سنجی/احراز هویت (authentication) رو به ما می‌ده، و این در بعضی شرایط می‌تونه حیاتی باشه، مثل زمانی که می‌خواید هویت شخصی ناشناس رو احراز کنید.

شخص پیامی رو با کلید خصوصی‌اش «امضا» می‌کنه، و شما با داشتن کلید عمومی‌اش قادر به احرازش هستید. در اینجا کمی وارد موضوع PGP می‌شیم—که جلوتر مفصل درموردش صحبت خواهیم کرد—اما قبل از اینکه من و ناداو ایوگی، از توسعه‌دهنده‌های قدیمی حوزهٔ بیت‌کوین، شروع به همکاری کنیم، نیاز بود هویت هم رو احراز کنیم. بهترین اقدام این بود که پیامی رو با مشخصات من و موضوع صحبتمون در اون لحظه امضا و ارسال کنه و من احراز کنم.

در اینجا، ناداو پیام رو امضا و برای من ارسال کرد، و من با واردکردن (import) کلید عمومی‌اش و صحت‌سنجی این پیام موفق به احراز هویتش برای خودم شدم.

بهتر می‌بود اگه زمان رو هم لحاظ می‌کرد، به ساعت هماهنگ جهانی (UTC).

gistfile1.txt Raw

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

I'm shesek on freenode, chatting with lmushix23 about eznode
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

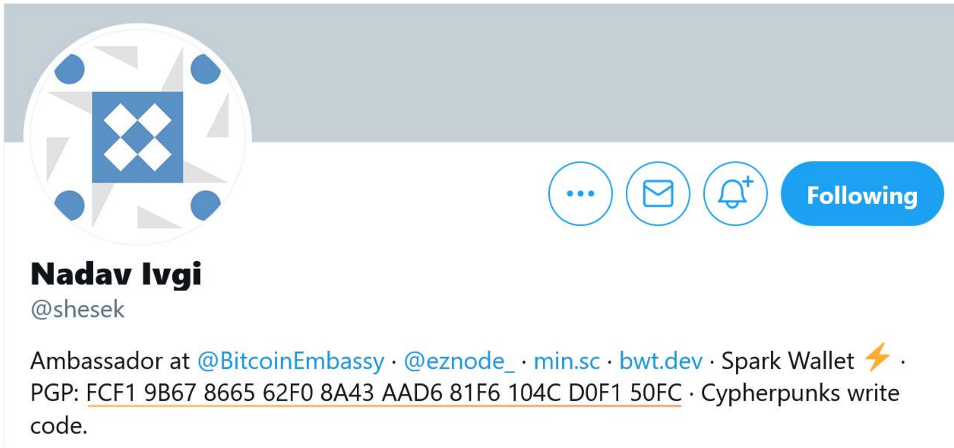
iQEcBAEBAgAGBQJgPWRZAAoJEIH2EEzQ8VD8PAEH/RmxTaZbfSgrCibnALBDTOfO
vCJW+av2v57BYX7ecPB81tgj4/uoQ99s87hpGRtjWJRixIFpJxWnoWxoZSRfVtRW
D0Ty2cqp7wV27SBgQP0o5pREYHVzvV0ka/9260pJXMCTbfyVpvA3zoNc1fRcdWBA
xu89fDa+y/SOEMQ5IHl/poI2REEwEQcBjBU/1WLAsyGsrkZ2uR3o/dwjTOb9VdfG
KC97EahJlEFLesVlfWy62hULFWxmkZVP3mbdO47P4CQUXE9LIztiFXFwXctmLIzK
VOCqr9S5jFEhP3nIViETZkIGW+RL6mLmDXd7qVGLZwyPRslgeyK3YVfNvH5Rvt4=
=2MGG
-----END PGP SIGNATURE-----
```

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Saeid> gpg --verify .\1f7483d020d72b07852790c755012e5b.txt
gpg: Signature made 3/2/2021
gpg:                using RSA key 81F6104CD0F150FC
gpg: Good signature from "Nadav Ivgi <nadav@shesek.info>" [unknown]
gpg:                 aka "Nadav Ivgi (Bitrated) <nadav@bitrated.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: FCF1 9B67 8665 62F0 8A43  AAD6 81F6 104C D0F1 50FC
PS C:\Users\Saeid> _
```



اثرانگشت کلید عمومی ناداو ایوگی

اصالت‌سنجی فایل‌ها، به‌ویژه در دنیای نرم‌افزار آزاد، بسیار مهمه. شما می‌خواید که مطمئن باشید نرم‌افزاری رو که دریافت می‌کنید صحیحه. اگه نرم‌افزار بیت‌کوین یا کیف پولی رو دانلود می‌کنید، مهمه که اصالتش رو قبل از استفاده احراز کنید، و این با مفهوم کلید عمومی و امضای دیجیتال ممکنه.

نکته: کلیدهای عمومی به‌طورمعمول بسیار بلندن، و این، کار رو برای انتقال و واردکردنشون سخت می‌کنه. ازاین‌رو، از اثرانگشت کلید عمومی استفاده می‌کنیم. ما می‌تونیم کلید عمومی خودمون رو با تابع رمزنگارانه خاصی هش کنیم و به اثرانگشت برسیم، که بسیار کوتاه‌تره. توجه کنید که همهٔ این‌ها، از تولید کلید عمومی و خصوصی گرفته تا ساختن اثرانگشت، در محیط نرم‌افزار اتفاق می‌افته. جلوتر به این نرم‌افزارها اشاره می‌کنم.

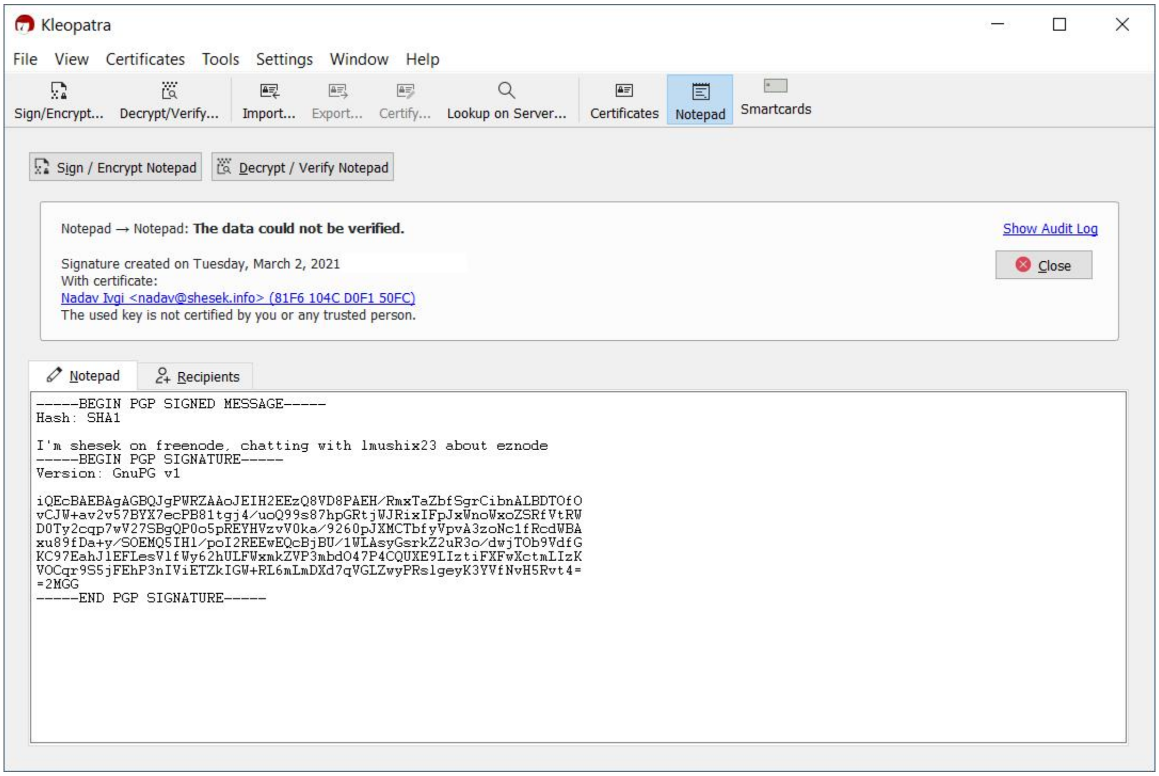
ممکنه اثرانگشت PGP بعضی رو در وبسایت یا پروفایل توئیترشون باشید. شما با داشتن این اثرانگشت می‌تونید به کلید عمومی‌شون برسید.

Fingerprint:	A6FFA9B242ADD0A68941005F021D780BDC0CC361
Long Key ID:	021D780BDC0CC361
Short Key ID:	DC0CC361

اثرانگشت کلید عمومی RSA من (چهل حرف و رقم). توجه کنید که شناسهٔ بلند کلید (long key ID) و شناسهٔ کوچک کلید (short key ID) به‌ترتیب شونزده و هشت رقم آخر اثرانگشتن. با داشتن هرکدوم از این‌ها می‌تونید کلید عمومی من رو پیدا و وارد کنید.

تولید کلید عمومی و خصوصی

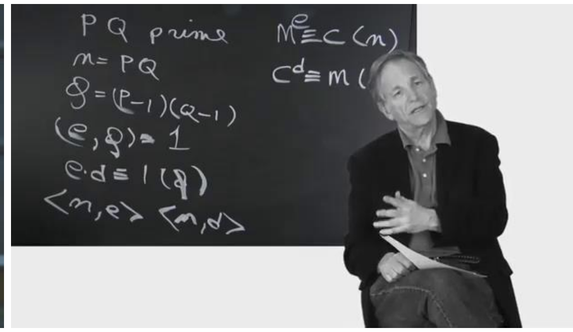
یکی از رایج‌ترین نرم‌افزارها GNU Privacy Guard یا GPG است. اگه کاربر ویندوز هستید، از Gpg4win استفاده کنید. لینک‌های دانلود برحسب سیستم عامل در سایت رسمی GnuPG قرار داده شدن.



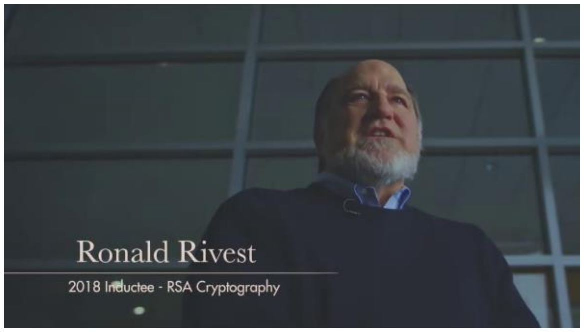
نرم‌افزار کلئوپاترا

سخن پایانی

ریاضی پشت کلید عمومی RSA بسیار جذابه اگه علاقه‌مند و کنجکاو به دونستنش هستید. توضیحش در قالب این مطلب کمی سخته، اما ویدئویی رو پیشنهاد می‌کنم که قدم‌به‌قدم توضیح می‌ده، و حتی اگه فکر می‌کنید در ریاضی قوی نیستید، می‌تونید نحوهٔ کارش رو درک کنید.



شرح RSA از زبان سازندگان اون در یوتیوب



داستان ریوست-شامیر-آدلمن در یوتیوب

از دید من، RSA، در کنار نوآوری‌های دیگه‌ای مثل پروتکل تبادل کلید دیفی-هلمن (Diffie–Hellman Key Exchange)، چهرهٔ رمزنگاری و ارتباطات رو برای همیشه تغییر داد. به لطف این افراد و تلاش‌هاشون، ما امروز فضای اینترنت و ارتباطات امن‌تری داریم. شما این‌طور فکر نمی‌کنید؟

راهنماهای مرتبط



حریم خصوصی در عصر دیجیتال



راهنمای جامع نرم‌افزار PGP